



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/379,791	08/24/1999	HIDEO SHIMIZU	04329.2151	1716

22852 7590 02/27/2004

FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER
LLP
1300 I STREET, NW
WASHINGTON, DC 20005

EXAMINER

SMITHERS, MATTHEW

ART UNIT	PAPER NUMBER
----------	--------------

2137

DATE MAILED: 02/27/2004

10

Please find below and/or attached an Office communication concerning this application or proceeding.

4

Office Action Summary

Application No.

09/379,791

Applicant(s)

SHIMIZU ET AL.

Examiner

Matthew B Smithers

Art Unit

2137

-- Th MAILING DATE of this communication appears on the cover sheet with the c rrespondenc address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 03 December 2003.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-14 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-14 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date 9.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____.

DETAILED ACTION

Information Disclosure Statement

The information disclosure statement filed 14 January 2004 has been placed in the application file and the information referred to therein has been considered as to the merits.

Response to Arguments

Applicant's arguments with respect to claims 1-14 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-14 are rejected under 35 U.S.C. 102(b) as being anticipated by U.S. 5,261,003 granted to Matsui.

Regarding claim 1, Matsui meets the claimed limitations as follows:

“A data processor in which at least one of encryption of a plain text to a cipher text by using an encryption key and decryption of a cipher text to a plain text by using a decryption key is performed, comprising:

a key converting section in which a plurality of key conversion functions which are involution functions, and which conducts key conversions to output extended keys for direct use of encrypting the plain text to the cipher text or decrypting the cipher text to the plain text based on one of the encryption key and the decryption key and results of key conversion of one of the encryption key and the decryption key are sequentially connected, and results of the key conversion are in an order or in another order reverse to the order transferred between the key conversion functions;" see column 5, lines 47-61 and column 6, lines 1-43

and a data randomize section in which at least one processing of encryption of the plain text to the cipher text and decryption of the cipher text to the plain text is performed by using the extended keys output from the key conversion section." see column 5, lines 8-12 and column 9, line 62 to column 10, line 9.

Regarding claim 2, Matsui meets the claimed limitations as follows:

"A data processor according claim 1, wherein the data randomize section includes a plurality of round functions which are involution functions and which perform at least one of encryption and decryption by using the extended keys, the plurality of round functions are sequentially connected, and results of the processing by the round functions are transferred in an order or in another order reverse to the order transferred between the plurality of round functions." see column 5, lines 8-12.

Regarding claim 3, Matsui meets the claimed limitations as follows:

"A data processor according to claim 1, wherein the key conversion functions take first keys and results of conversion of the first keys as objects to be processed in the key

conversion, and perform the key conversion by using a second key.” see column 5, lines 47-61 and column 6, lines 1-43 and Figure 1.

Regarding claim 4, Matsui meets the claimed limitations as follows:

“A data processor according to claim 3, wherein the second key is included in at least one of the encryption key and the decryption key.” see column 5, lines 47-61 and column 6, lines 1-43 and Figure 1.

Regarding claim 5, Matsui meets the claimed limitations as follows:

“A data processor according to claim 4, wherein the second key has different types of keys, at least one of the encryption key and the decryption key includes the different types of keys and at least one of the encryption key and the decryption key is variable in length.” see column 5, lines 47-61 and column 6, lines 1-43 and Figure 1.

Regarding claim 6, Matsui meets the claimed limitations as follows:

“A data processor according to claim 2, wherein the key conversion functions include round functions that are the same as that of the data randomize section.” see column 5, lines 47-61 and column 6, lines 1-43 and Figure 1.

Regarding claim 7, Matsui meets the claimed limitations as follows:

“A communication system comprising:

one communication device which includes a data processor according to claim 1 and holds one key which serves as the encryption key and the decryption key; and

another device which includes a data processor according to claim 1 and holds other key which serves as the encryption key and the decryption key, and which is a

Art Unit: 2137

result of key conversion of the one key in the key conversion section of the another device.” see Abstract.

Claim 8 is a computer readable medium claim that is substantially equivalent to data processor claim 1. Therefore claim 8 is rejected by a similar rationale.

Claims 9-13 are computer readable medium claims that are substantially equivalent to data processor claims 2-6. Therefore claims 9-13 are rejected by a similar rationale.

Regarding claim 14, Matsui meets the claimed limitations as follows:

“A data transformation apparatus comprising: a key transformation section for outputting a second key and a third key by using an involution function based on inputted first key and for outputting the first key and a fourth key by using the involution function based on inputted second key, wherein the third key is directly used for encrypting plain text to cipher text when first data is transformed to second data and the fourth key is used for decrypting the cipher text to the plain text when the second data is transformed to the first data.” see column 5, lines 47-61 and column 6, lines 1-43 and Figure 1.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

A. Torigai et al (6,038,321) discloses a communications system encrypting variable length data with a random number to produce a variable-length random number sequence.

B. Matsui (5,488,661) discloses a communications system using extended keys.

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

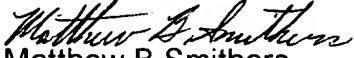
A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew B Smithers whose telephone number is (703) 308-9293. The examiner can normally be reached on Monday-Friday (9:00-5:30) EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A Morse can be reached on (703) 308-4789. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Art Unit: 2137

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).


Matthew B Smithers
Primary Examiner
Art Unit 2137